noyb – European Center for Digital Rights
Goldschlagstraße 172/4/3/2
1140 Vienna
AUSTRIA

Dear Commissioner Didier Reynders,
Dear Secretary Gina Raimondo,
Dear Pauline Dubarry,
Dear EDPB Chair Andrea Jelinek,
Dear LIBE Chair Juan Fernando López Aguilar,

Open Letter

Announcement of a New EU-US Personal Data Transfer Framework

We take note of the announcement of an agreement on principle for a new Trans-Atlantic Data Privacy Framework. We understand that the future deal "agreed in principle" is mainly based on a political agreement between Commission President von der Leyen and US President Joe Biden, but is not the result of material changes to U.S. law in response to the CJEU's judgement. This approach seems to repeat the "Privacy Shield" agreement and is deeply concerning.

We are aware that the announcement only outlines rough ideas and headlines, but that the final text still needs to be negotiated. The following *preliminary* observations are therefore based on the limited political announcement and further details that were informally shared with stakeholders in various public or semi-public formats by the EU and the US.

Based on these statements, we understand that the US has rejected any material protections for non-US persons and is continuing to discriminate against non-US persons by refusing baseline protections, such as judicial approval of individual surveillance measures.

We understand that the envisioned deal will largely rely on US executive orders. Having worked on this matter with US surveillance experts and lawyer, such executive orders seem to be structurally insufficient to meet the requirements of the CJEU.

Based on the known cornerstones, we warn negotiators on both sides of the Atlantic, the Council of the EU, the EDPB and the LIBE Committee of the European Parliament that the announced framework risks sharing the same fate as its two predecessors in front of the CJEU unless substantive (legislative) reforms are conducted in the United States.

We call on the negotiators to continue working for a long-standing, privacy preserving solution for trans-Atlantic flows to avoid a "*Schrems III*" decision. The current approach may cause further legal uncertainty for citizens and businesses for years to come - a fear that was also voiced by industry representatives in reaction to the "agreement in principle".

We are fully aware that this is everything but an easy task, but the investment in getting it *right* would not only ensure that this matter is solved in the long run, but also benefit citizens and the economy on both sides.

To reach that goal, we present the following more detailed observations and recommendations:

(1) Applying a correct proportionality test on US surveillance law under Article 8 CFR

We understand that the US negotiators do not plan to seek amendments to US statutory law in relation to material surveillance, but plan to essentially replace Presidential Policy Directive 28 (PPD-28) on Signals Intelligence Activities with a new executive order that would include the words "*necessary and proportionate*".

It seems that the European Commission aims at finding that these words in a US Executive Order should be seen as equivalent to the EU proportionality test in Article 52 of the Charter of Fundamental Rights (CFR).

However, it is hard to see how existing US surveillance can be "*necessary and proportionate*" under European law if the CJEU has explicitly found the opposite in two judgements.

This approach seems to be insufficient for at least the following reasons:

- In both CJEU judgements ("*Schrems I*" and "*Schrems II*"), the Court has clearly held that US surveillance laws and practices violate Article 7, 8 and 47 of the Charter of Fundamental Rights. The CJEU has even explicitly found these laws and practices *not* to be "*necessary and proportionate*".
- The "*Schrems II*" ruling was delivered taking PPD28 (as the relevant executive directive at the time) into account. As the European Commission and the US Government have argued before the CJEU, PPD-28 already include the wording "*as tailored as feasible*", which the Commission has interpreted as equivalent to proportionality under Article 52 CFR. The CJEU has rejected this idea. We fail to see how laws and practices that the CJEU has explicitly found *not* to be "*necessary and proportionate*" could suddenly convince the CJEU if they are relabeled "*necessary and proportionate*" instead of "*as tailored as feasible*".
- We understand that, while the US may adopt these words, it has not agreed to limiting surveillance of non-US data subjects in any material way. Specifically, the US has not announced any intention to limit or revise surveillance practices conducted under the laws and programs (FISA 702, EO 12,333, "PRISM" and "Upstream") specifically mentioned by the CJEU in its ruling. The US has also not indicated it would conduct any changes to put an end to its bulk surveillance practices. The surveillance programs seem to continue as they are. The CJEU has conducted a proportionality test under Article 52 CFR and concluded that the US surveillance practices failed that test. If the US was to integrate the concept of "*necessity and proportionality*", this would mean stopping or severely limiting these surveillance practices. The negotiators are clear that this is not intended.
- The negotiators therefore seem to merely copy the *words* of the CFR and CJEU case law to a US executive order, but will likely apply a different *meaning* than the CJEU, as this would otherwise have to lead to a stop of the Upstream and Downstream (previously "PRISM") programs under Section 702 of the Foreign Intelligence Surveillance Act (FISA), and an end to bulk surveillance under Executive Order 12,333.
- We are further concerned that executive orders typically do not confer third-party rights. It seems that even if a "*necessary and proportionate*" test in line with Article 52 CFR would be implemented in an executive order, any data subject may not be able to enforce such limitations in court.

In summary, this approach seems to merely satisfy the political, diplomatic and PR requirements of both sides, but seems to ignore the fact that the CJEU has already found that US surveillance is not "necessary and proportionate" and the US will continue these practices.

(2) Creating meaningful judicial redress under Article 47 CFR

We understand that the US negotiators do not plan to amend US law to create avenues for judicial redress for EU data subjects.

Instead, the US executive should form a new "body" within the executive branch (similar to the previous "Ombudsperson" but under the authority of the Advocate General) that will deal with potential violations of US law and executive orders. This body called the "Data Protection Review Court" will - contrary to the name - not be a "Court" but an executive body. It will be part of the executive branch, with limited independence.

We understand that EU data subjects would not be able to access information about potential surveillance operations concerning them during proceedings and they would not be able to appeal decisions from this "Court" to fully independent judicial body established under Article 3 of the US Constitution.

This approach seems to violate the CJEU case law in at least the following aspect:

- The proposed solution does not provide for *judicial* redress, but for a redress body within the executive branch – similar to the Ombudsperson, which the CJEU found not just to be disproportionate, but a breach of the essence of Article 47 CFR. Just naming an executive body a "Court" does not create *judicial* redress. The approach seems to be better described as an "Ombudsperson Plus".
- It is hard to see how this new body would fulfill the formal requirements of a court or tribunal under Article 47 CFR, especially when compared to ongoing cases and standards applied within the EU (for example in Poland and Hungary). The CJEU would be asked to apply a "high" Article 47 CFR standard within the EU, but a "low" Article 47 CFR standard for a US "Data Protection Review Court". It would be the European Commission that would have to convince the CJEU of these different standards under Article 47 CFR.
- We understand that this new "Court" will continue to operate like the current "Ombudsperson" and will *neither confirm nor deny* if a person was subject to surveillance and if there was a breach of US law. It is our understanding that the data subject will have no direct or indirect option to see evidence, request discovery, question the opponent or receive a reasoned judgment. This will make it a "rubber stamp" institution, with no practical relevance.
- This "rubber stamp" approach will also limit the options for any potentially envisaged appeal to any secondary body: If the "Data Protection Review Court" is bound to send a prescribed standard answer, we fail to see that there is room for any informed, meaningful material appeal. If there is only *one* possible predefined outcome in each case, there seems to be hardly any case where a citizen may raise an error, as there seems to be only one possible answer.
- There are fundamental questions if US doctrines like "state secrets" will apply for these bodies and further limit any option for a fair hearing. We understand that the US government will continue to rely on these doctrines.

In summary, we fail to see how this new "Court" would be compliant with Article 47 CFR, especially in the light of recent CJEU case law on US surveillance, but also in light of CJEU case law on judicial redress and the rule of law in EU Member States. It seems the CJEU would have to develop a separate Article 47 CFR test for the US, to find that an executive body producing rubber stamp responses is indeed a form of judicial redress. We fail to see how such a development in CJEU case law is remotely realistic or even desirable.

(3) The need to update commercial privacy protections

In addition to the shortcomings of the announced agreement in principle linked to the lack of reforms on US surveillance and laws, we also caution the EU negotiators about the need to update the commercial data protection obligations under any future deal.

We are concerned that the EU and US negotiators do not seem to plan any updates to the Privacy Shield Principles itself. We understand that the Privacy Shield Principles and certifications would not be touched or even renamed. This is hugely problematic, as the principles are largely based on the "Safe Harbor" principles from 2000, with only minor updates in 2016. They are not in line with the GDPR requirements, which became applicable in 2018. In fact, the Privacy Shield Principles even refer to the non-longer applicable Directive 95/46/EC, and not the GDPR.

We highlight here a few examples of some of many deficiencies of the Privacy Shield Principles and where they depart from the GDPR:

- The Privacy Shield Principles do not have a general requirement for a legal basis, as under Article 6(1) GDPR and Article 8(2) of the Charter of Fundamental Rights. In fact, there is only a so-called "notice & choice" approach with a right to reject (opt-out). Especially because the principles usually apply to sub-processors, with no direct contact with a data subject, there seems to be hardly a realistic scenario, where a data subject would even be notified about problematic processing.
- The Privacy Shield Principles do not require data processing to be "necessary", as required by Article 5(1)(c) GDPR and Article 52(1) CFR, but only "relevant".
- Most elements of the Right to Access under Article 15 GDPR and Article 8(2) of the Charter of Fundamental Rights are not reflected in the Privacy Shield Principles.
- The redress mechanism provided under the Principles is based on private arbitration, a system that is banned in relation to consumers in the EU since Directive 93/13/EEC. The private arbitration services are paid by the US company and do not have the necessary "supervision and detection" mechanisms or powers that even remotely resemble the powers of EU supervisory authorities under Article 58 GDPR. There are multiple steps for any arbitration ruling to be actually enforceable under US law.

There are countless further examples, where the Privacy Shield Principles are not "essentially equivalent" to the GDPR and therefore allow US competitors to operate on the European market, without complying with EU law. Even if the matters of US surveillance would be solved, any new agreement may be invalidated by the CJEU on the basis that the Privacy Shield Principles are not at all "essentially equivalent" to the GDPR.

The future of international data transfers

We are sorry to see, that the negotiators have not used this opportunity to ensure that the human rights to privacy and data protection are protected on both sides of the Atlantic and independent of geographic location or citizenship. We are deeply convinced that a global internet and the free flow of personal data is only possible if protections are not based on historic and nationalistic concepts, such as citizenship. While the GDPR and Article 7, 8 and 47 CFR are human rights and apply to any user, independent of national ties, FISA 702 and the relevant executive orders in the US continue to follow an archaic idea of "US persons" and "non-US persons".

This is not just causing violations of human rights, but also seems to undermine the alleged aims of these surveillance laws: We know that most current dangers (such as homegrown terrorism, espionage and alike) are not based on citizenship of the target.

We call upon the negotiators and other relevant stakeholders, including such as the US tech industry, to call traditional nationalistic concepts into question. If the internet should not know national borders, our privacy rights and surveillance laws must equally overcome nationalistic concepts. One option would be international agreements among democratic nations.

Chapter 5 of the GDPR already allows for a free flow of data – if protections are "essentially equivalent". We regret that national surveillance laws in the US and the EU still hold on to concepts like citizenship and so far lack modern interoperability clauses.

This conflict of (interoperable) privacy protections and (nationalistic) surveillance laws hinder international data flows, trade, and convergence.

Reaction to any new adequacy decision

As our litigation is always aimed at ensuring a durable solution that both protects user data and allows free data flows, we would be the first to applaud any such outcome. We are still hopeful that any final text can overcome the shortcomings highlighted in this letter and we encourage negotiators on both sides of the Atlantic to advance much-needed reforms on US law.

In the absence of these legislative changes, we are concerned that any future agreement would be (again) based on political hopes instead of legal realities. We are especially concerned that the European Commission may knowingly adopt another unlawful adequacy decision with the aim of undermining the CJEU's judgements. This is often referred to as "buying another couple of years". This may not only lead to an endless ping-pong between Brussels and Luxembourg, but also threatens the trust in the rule of law and the CFR on the European level.

In light of the foregoing, *noyb* is prepared to challenge any final adequacy decision that would fail to provide the needed legal certainty. In case such litigation is indeed necessary, we will especially focus on a quick and efficient path to the CJEU to reach a rapid decision. We hope that this will ensure a shorter period of legal uncertainty in the case of any ill-conceived political agreement.

Such a challenge may include a request for the CJEU to suspend the application of any third version of a US adequacy decision. Such an option is foreseen in Article 278 TFEU and could ensure that the European Commission is not undermining the CJEU by passing further unlawful adequacy decisions in an attempt to outpace the CJEU's review of the same.

We hope that these *preliminary* observations are useful for you. We are available to you in case you have any questions or would like to provide us with further clarifications on the envisioned new deal.

Sincerely,

Max Schrems

Honorary Chairman, noyb